Available online at www.sciencedirect.com
ScienceDirect
Discrete Mathematics 309 (2009) 1347–1356
DISCRETE MATHEMATICS
www.elsevier.com/locate/disc

Hadamard 2-(63,31,15) designs invariant under the dihedral group of order 10[☆]

Zlatka Mateva[a], Svetlana Topalova[b,*]

[a] Department of Mathematics, Technical University Varna, Bulgaria, 1 Studentska St., 9010 Varna, Bulgaria
[b] Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, P.O. Box 323, 5000 Veliko Tarnovo, Bulgaria

Received 27 June 2007; received in revised form 9 January 2008; accepted 3 February 2008
Available online 19 March 2008

Abstract

All Hadamard 2-(63,31,15) designs invariant under the dihedral group of order 10 are constructed and classified up to isomorphism together with related Hadamard matrices of order 64. Affine 2-(64,16,5) designs can be obtained from Hadamard 2-(63,31,15) designs having line spreads by Rahilly's construction [A. Rahilly, On the line structure of designs, Discrete Math. 92 (1991) 291–303]. The parameter set 2-(64,16,5) is one of two known sets when there exists several nonisomorphic designs with the same parameters and p-rank as the design obtained from the points and subspaces of a given dimension in affine geometry $AG(n, p^m)$ (p a prime). It is established that an affine 2-(64,16,5) design of 2-rank 16 that is associated with a Hadamard 2-(63,31,15) design invariant under the dihedral group of order 10 is either isomorphic to the classical design of the points and hyperplanes in $AG(3, 4)$, or is one of the two exceptional designs found by Harada, Lam and Tonchev [M. Harada, C. Lam, V.D. Tonchev, Symmetric (4, 4)-nets and generalized Hadamard matrices over groups of order 4, Designs Codes Cryptogr. 34 (2005) 71–87].

Keywords: Classification; Hadamard design; Hadamard matrix; Automorphism; Line spread

1. Introduction

For basic concepts and notations concerning Hadamard matrices and combinatorial designs refer, for instance, to [1,2,6,30], or [36].

Let $V = \{P_i\}_{i=1}^{v}$ be a finite set of *points*, and $\mathcal{B} = \left\{B_j\right\}_{j=1}^{b}$ a finite collection of k-element subsets of V, called *blocks*. $D = (V, \mathcal{B})$ is a *design* with parameters t-(v,k,λ) if any t-subset of V is contained in exactly λ blocks of $\mathcal{B}$.

The incidence matrix of a design is a (0, 1) matrix with v rows and b columns, where the element of the i-th row and j-th column is 1 if $P_i \in B_j$ ($i = 1, 2, \ldots, v$; $j = 1, 2, \ldots, b$) and 0 otherwise. The design is completely determined by its incidence matrix.

Two designs are *isomorphic* if there exists a one-to-one correspondence between the point and block sets of the first design and the point and block sets of the second design, and if this one-to-one correspondence does not change

☆ Some of the results were briefly announced at the International Conference Pioneers of Bulgarian Mathematics, Sofia, July 8–10, 2006.

* Corresponding author.
E-mail addresses: ziz@abv.bg (Z. Mateva), svetlana@moi.math.bas.bg (S. Topalova).

0012-365X/$ - see front matter
doi:10.1016/j.disc.2008.02.001

the incidence, i.e. if the incidence matrix of the first design can be obtained from the incidence matrix of the second one by permuting rows and columns.

A design is *symmetric* if the number of blocks equals the number of points. The *dual* of a symmetric design is a design with the same parameters, whose points correspond to blocks of the initial design, and blocks to the points. A symmetric design is *selfdual* if it is isomorphic to its dual.

An *automorphism* is an isomorphism of the design to itself, i.e. a permutation of the points that transforms blocks into blocks. The set of all automorphisms of a design form a group called its *full group of automorphisms*. Each subgroup of this group is a group of automorphisms of the design.

A *resolution* is a partition of the collection of blocks into *parallel classes*, such that each point is in exactly one block of each parallel class. The design is *resolvable* if it has at least one resolution. An *affine* (or *affine resolvable*) design is a resolvable design such that every two blocks that belong to different parallel classes share the same number of points.

A *Hadamard matrix of order n* is an $n \times n (\pm 1)$-matrix satisfying $HH^t = nI$ (its rows are pairwise orthogonal). Two Hadamard matrices are *equivalent* if one can be transformed into the other by a series of row or column permutations and negations. We call a Hadamard matrix *selfdual* if it is equivalent to its transpose. An *automorphism* of a Hadamard matrix is an equivalence to itself.

Each Hadamard matrix can be normalized, i.e. replaced by an equivalent Hadamard matrix whose first row and column entries are 1-s. Deleting the first row and column of a normalized Hadamard matrix of order $4m$, and replacing -1-s by 0-s, one obtains a symmetric 2-($4m-1$,$2m-1$,$m-1$) design which is called a Hadamard 2-design.

A line in a design through a pair of points x, y is the intersection of all blocks containing x and y. A line spread is a partition of the point set of a design into disjoint lines. The maximal size of a line in a Hadamard 2-design is 3.

Hadamard matrices have extremely interesting combinatorial properties, and various applications [6,7,30]. There has been a continuous interest in their studies. Hadamard matrices of orders up to 28 have been fully classified [1,17, 20,21,31]. Only partial classifications are available for bigger orders (see for instance [4,8,11,12,32,34]), because the computational complexity of the classification problem rises exponentially.

Classification methods similar to those used in the present work have been used, for instance, in [4,9,19,33,34,38].

Lower bounds on the number of Hadamard designs and matrices containing Hadamard designs of smaller order, are established in [23,24]. According to these bounds there are at least 31! non isomorphic 2-(63,31,15) designs. The construction of a great number of Hadamard matrices of orders divisible by 8 by doubling constructions was announced in [13].

Hamada formulated a conjecture [14] according to which the design obtained from the points and subspaces of a given dimension in affine geometry $AG(n, p^m)$ (p a prime) has minimal p-rank, and all the other designs with the same parameters have greater p-rank. Counterexamples to this conjecture are given by five 3-(32,8,7) designs [35] and three 2-(64,16,5) designs [15,27]. In this aspect further investigations on non geometric 2-(64,16,5) designs of minimum rank and the corresponding by Rahilly's construction [29] Hadamard designs are of particular interest [37]. The two Hadamard 2-(63,31,15) designs, which correspond to the three known 2-(64,16,5) designs of rank 16 are invariant under the dihedral group of order 10. This inspired the present classification of all Hadamard 2-(63,31,15) designs invariant under the dihedral group of order 10.

In [22] 394 Hadamard matrices of order 64 with two circulant cores were constructed. They all have 2-ranks greater than 16. In [9] 38 2-(63,31,15) designs with a nonabelian automorphism group of order 155 were constructed. Among them there are 11 designs of 2-rank not greater than 16, i.e. the point-hyperplane design in $PG(5, 2)$, and 10 designs of rank 12, which do not yield 2-(64,16,5) designs of minimum rank. We do not know other constructions of 2-(63,31,15) by prescribed automorphisms. For these parameters construction of all the designs with some smaller prime automorphism is a long time consuming task.

We construct 8330 non isomorphic 2-(63,31,15) designs invariant under the dihedral group of order 10 and classify them with respect to the automorphism group order, and to their 2-rank. We also establish that there are 1691 equivalence classes of the related Hadamard matrices of order 64 and present their classification with respect to the automorphism groups.

From the 2-(63,31,15) designs of 2-rank at most 16, we next construct all line spreads, which correspond to 2-(64,16,5) designs of rank at most 16. They yield the three 2-(64,16,5) designs of rank 16 known by now [15,27], and no new ones.

2. On the automorphisms of 2-(63,31,15) designs

Theorem 1 (*Brauer 1941, Parker 1957, see [2], p. 36, I.4.8*). *For an automorphism of a symmetric design the number of fixed points equals the number of fixed blocks.*

2.1. Automorphisms of prime orders of 2-(63,31,15) designs

Theorem 2. *All possible prime divisors of the order of the automorphism group of a* 2-(63, 31, 15) *design are* 2, 3, 5, 7 *and* 31.

Proof. If a 2-(v, k, λ) design possesses an automorphism of a prime order p, then $p \leq k$ or $p|v$. (Otherwise there should exist fixed points and blocks, all the fixed points should be in fixed blocks, and all the fixed blocks should only contain fixed points, thus forming a 2-(v, k, λ), i.e. all the points and blocks will be fixed.) Thus $p = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31$ are the only possible prime orders of automorphisms of this design.

(a) Consider $p = 11, 13$. Suppose there exists an automorphism of order p, fixing $f \geq 63 \bmod p$ points. In this case fixed blocks may contain the points of 0,1, or 2 non fixed point orbits, and respectively k,$k - p$ or $k - 2p$ fixed points, i.e. $f \geq k - 2p$. It follows that for $p = 11$, $f \geq 19$ and for $p = 13$, $f \geq 11$. Two blocks are both incident with $\lambda = 15$ points, and thus the points of each pair of nontrivial point orbits should be in at most one fixed block. It follows that there are fixed blocks containing $k = 31$ fixed points, i.e $f \geq 31$. Yet for $f \geq 31$ there are more than 16 fixed blocks containing $k = 31$ fixed points, which is impossible because for each pair of points of the design there are 16 blocks not incident with any of the two points.

(b) Consider $p = 17, 19, 23, 29$. Suppose there exists an automorphism of order p, fixing $f \geq 63 \bmod p$ points. In this case fixed blocks may contain points of 0 or 1 non fixed point orbit, and respectively k or $k - p$ fixed points. Yet $\lambda = 15$, and thus the points of each nontrivial point orbit should be in at most one fixed block. In a way similar to that in (a) it follows that there are more than 16 fixed blocks containing $k = 31$ fixed points, which is impossible. □

2.2. Automorphisms of order 5 of 2-(63,31,15) designs

Theorem 3. *An automorphism of order* 5 *of a* 2-(63, 31, 15) *design fixes* 3 *points and* 3 *blocks.*

Proof. Suppose a 2-(63,31,15) design possesses an automorphism of order 5 fixing $f > 3$ points and blocks. An automorphism of a symmetric design can fix at most half of the points [5,10,25]. That is why $f = 8, 13, 18, 23, 28$. Let $w = (63 - f)/5$ be the number of nontrivial point/block orbits. The nontrivial orbit part of the incidence matrix of D is:

$$\begin{pmatrix} A_{1,1} & A_{1,2} & \dots & A_{1,w} \\ A_{2,1} & A_{2,2} & \dots & A_{2,w} \\ \dots & \dots & \dots & \dots \\ A_{w,1} & A_{w,2} & \dots & A_{w,w} \end{pmatrix}$$

where $A_{i,j}$, $i, j = 1, 2, \dots, w$ are circulant matrices of order 5. Let $n_{i,j}$, $i, j = 1, 2, \dots w$, be the number of 1's in a row of $A_{i,j}$, s_i the number of fixed blocks incident with the points of the i-th nontrivial point orbit, and s_{i_1,i_2} the number of fixed blocks, containing the pair of point orbits (i_1, i_2). The following equations hold for the matrix $N = (n_{i,j})_{w\times w}$

$$\sum_{j=1}^{w} n_{i,j} = 31 - s_i, \quad i = 1, 2, \dots, w \tag{1}$$

$$\sum_{j=1}^{w} n_{i,j}^2 = 91 - 5s_i, \quad i = 1, 2, \dots, w \tag{2}$$

$$\sum_{i=1}^{w} n_{i_1,j} n_{i_2,j} = 75 - 5s_{i_1,i_2}, \quad i_1, i_2 = 1, 2, \dots, w, i_1 \neq i_2. \tag{3}$$

The subsystem of (1) and (2) only has integer solutions for $f = 8$, but they cannot be extended to integer solutions of the whole system.

2.3. On 2-(63,31,15) designs with automorphisms of order 5

We can assume that the design possesses an automorphism α of order 5 transforming the points and blocks as

$$(1, 2, 3, 4, 5)(6, 7, 8, 9, 10)...(56, 57, 58, 59, 60)(61)(62)(63).$$

There is an incidence matrix of the design, which can be presented by means of four submatrices:

$$\begin{pmatrix} A & H \\ F & C \end{pmatrix},$$

where $A = (a_{ij})_{12\times 12}$ is a symmetric matrix corresponding to the non-fixed part. The elements of A are circulant matrices a_{ij} of order 5. Matrices H, F, and C correspond to elements fixed by α. An example of such a design is presented in Fig. 1.

Without loss of generality we set

$$C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Each element f_{ij} of F is $p = (1, 1, 1, 1, 1)$ if the i-th fixed point occurs in the j-th non-fixed orbit of blocks and $o = (0, 0, 0, 0, 0)$ otherwise. There are 4 possibilities for F

$$a = \begin{pmatrix} p & p & p & p & p & p & o & o & o & o & o & o \\ p & p & p & o & o & o & p & p & p & o & o & o \\ p & p & p & o & o & o & o & o & o & p & p & p \end{pmatrix}$$

$$b = \begin{pmatrix} p & p & p & p & p & p & o & o & o & o & o & o \\ p & p & p & o & o & o & p & p & p & o & o & o \\ o & o & o & p & p & p & p & p & p & o & o & o \end{pmatrix}$$

$$c = \begin{pmatrix} p & p & p & p & p & p & o & o & o & o & o & o \\ p & p & p & o & o & o & p & p & p & o & o & o \\ p & o & o & p & p & o & p & p & o & p & o & o \end{pmatrix}$$

$$d = \begin{pmatrix} p & p & p & p & p & p & o & o & o & o & o & o \\ p & p & p & o & o & o & p & p & p & o & o & o \\ p & p & o & p & o & o & p & o & o & p & p & o \end{pmatrix}.$$

The four possibilities for H are given by a transpose of the upper matrices. There are 16 ways to combine the matrices H and F, but the design is symmetric, so only 10 can be considered: (a, a^T), (a, b^T), (a, c^T), (a, d^T), (b, b^T), (b, c^T),(b, d^T), (c, c^T), (c, d^T), (d, d^T). The 10 different possibilities for this fixed part impose different requirements on the number of ones in each circulant of the nontrivial orbit part A. Let $m_{i,j}$, $i, j = 1, 2, \dots 12$, be the number of 1's in a row of $a_{i,j}$, s_i the number of fixed blocks incident with the points of the i-th nontrivial point orbit, and s_{i_1,i_2} the number of fixed blocks, containing the pair of point orbits (i_1, i_2). The following equations hold for the matrix $M = (m_{i,j})_{12\times 12}$

$$\sum_{j=1}^{12} m_{i,j} = 31 - s_i, \quad i = 1, 2, \dots, 12 \tag{4}$$

$$\sum_{j=1}^{12} m_{i,j}^2 = 91 - 5s_i, \quad i = 1, 2, \dots, 12 \tag{5}$$

$$\sum_{i=1}^{12} m_{i_1,j} m_{i_2,j} = 75 - 5s_{i_1,i_2}, \quad i_1, i_2 = 1, 2, \dots, 12, i_1 \neq i_2. \tag{6}$$

We first construct all inequivalent solutions for the matrix M for all the ten cases for the fixed part. In three of them, namely (a, a^T), (a, b^T), (b, b^T), M has an additional symmetry, which we use to find the solutions for M in

10000 01000 00100 00010 0 0001	11001 11100 01110 00111 10011	10110 01011 10101 11010 01101	10000 01000 00100 00010 00001	11001 11100 01110 00111 10011	10110 01011 10101 11010 01101	10000 01000 00100 00010 00001	10110 01011 10101 11010 01101	11001 11100 01110 00111 10011	10000 01000 00100 00010 00001	10110 01011 10101 11010 01101	11001 11100 01110 00111 10011	111 111 111 111 111
10110 01011 10101 11010 0 1101	10000 01000 00100 00010 00001	11001 11100 01110 00111 10011	10110 01011 10101 11010 01101	10000 01000 00100 00010 00001	11001 11100 01110 00111 10011	11001 11100 01110 00111 10011	10000 01000 00100 00010 00001	10110 01011 10101 11010 01101	11001 11100 01110 00111 10011	10000 01000 00100 00010 00001	10110 01011 10101 11010 01101	111 111 111 111 111
11001 11100 01110 00111 1 0011	10110 01011 10101 11010 01101	10000 01000 00100 00010 00001	11001 11100 01110 00111 10011	10110 01011 10101 11010 01101	10000 01000 00100 00010 00001	10110 01011 10101 11010 01101	11001 11100 01110 00111 10011	10000 01000 00100 00010 00001	10110 01011 10101 11010 01101	11001 11100 01110 00111 10011	10000 01000 00100 00010 00001	111 111 111 111 111
10000 01000 00100 00010 0 0001	11001 11100 01110 00111 10011	10110 01011 10101 11010 01101	01111 10111 11011 11101 11110	00110 00011 10001 11000 01100	01001 10100 01010 00101 10010	01111 10111 11011 11101 11110	00110 00011 10001 11000 01100	01001 10100 01010 00101 10010	10000 01000 00100 00010 00001	11001 11100 01110 00111 10011	10110 01011 10101 11010 01101	100 100 100 100 100
10110 01011 10101 11010 0 1101	10000 01000 00100 00010 00001	11001 11100 01110 00111 10011	01001 10100 01010 00101 10010	01111 10111 11011 11101 11110	00110 00011 10001 11000 01100	01001 10100 01010 00101 10010	01111 10111 11011 11101 11110	00110 00011 10001 11000 01100	10110 01011 10101 11010 01101	10000 01000 00100 00010 00001	11001 11100 01110 00111 10011	100 100 100 100 100
11001 11100 01110 00111 1 0011	10110 01011 10101 11010 01101	10000 01000 00100 00010 00001	00110 00011 10001 11000 01100	01001 10100 01010 00101 10010	01111 10111 11011 11101 11110	00110 00011 10001 11000 01100	01001 10100 01010 00101 10010	01111 10111 11011 11101 11110	11001 11100 01110 00111 10011	10110 01011 10101 11010 01101	10000 01000 00100 00010 00001	100 100 100 100 100
01111 10111 11011 11101 1 1110	00110 00011 10001 11000 01100	01001 10100 01010 00101 10010	10000 01000 00100 00010 00001	11001 11100 01110 00111 10011	10110 01011 10101 11010 01101	01111 10111 11011 11101 11110	00110 00011 10001 11000 01100	01001 10100 01010 00101 10010	10000 01000 00100 00010 00001	11001 11100 01110 00111 10011	10110 01011 10101 11010 01101	010 010 010 010 010
01001 10100 01010 00101 1 0010	01111 10111 11011 11101 11110	00110 00011 10001 11000 01100	10110 01011 10101 11010 01101	10000 01000 00100 00010 00001	11001 11100 01110 00111 10011	01001 10100 01010 00101 10010	01111 10111 11011 11101 11110	00110 00011 10001 11000 01100	10110 01011 10101 11010 01101	10000 01000 00100 00010 00001	11001 11100 01110 00111 10011	010 010 010 010 010
00110 00011 10001 11000 0 1100	01001 10100 01010 00101 10010	01111 10111 11011 11101 11110	11001 11100 01110 00111 10011	10110 01011 10101 11010 01101	10000 01000 00100 00010 00001	00110 00011 10001 11000 01100	01001 10100 01010 00101 10010	01111 10111 11011 11101 11110	11001 11100 01110 00111 10011	10110 01011 10101 11010 01101	10000 01000 00100 00010 00001	010 010 010 010 010
01111 10111 11011 11101 1 1110	00110 00011 10001 11000 01100	01001 10100 01010 00101 10010	01111 10111 11011 11101 11110	00110 00011 10001 11000 01100	01001 10100 01010 00101 10010	10000 01000 00100 00010 00001	10110 01011 10101 11010 01101	11001 11100 01110 00111 10011	10000 01000 00100 00010 00001	10110 01011 10101 11010 01101	11001 11100 01110 00111 10011	001 001 001 001 001
01001 10100 01010 00101 1 0010	01111 10111 11011 11101 11110	00110 00011 10001 11000 01100	01001 10100 01010 00101 10010	01111 10111 11011 11101 11110	00110 00011 10001 11000 01100	11001 11100 01110 00111 10011	10000 01000 00100 00010 00001	10110 01011 10101 11010 01101	11001 11100 01110 00111 10011	10000 01000 00100 00010 00001	10110 01011 10101 11010 01101	001 001 001 001 001
00110 00011 10001 11000 0 1100	01001 10100 01010 00101 10010	01111 10111 11011 11101 11110	00110 00011 10001 11000 01100	01001 10100 01010 00101 10010	01111 10111 11011 11101 11110	10110 01011 10101 11010 01101	11001 11100 01110 00111 10011	10000 01000 00100 00010 00001	10110 01011 10101 11010 01101	11001 11100 01110 00111 10011	10000 01000 00100 00010 00001	001 001 001 001 001
11111 00000 0 0000	11111 00000 00000	11111 00000 00000	00000 11111 00000	00000 11111 00000	00000 11111 00000	00000 00000 11111	00000 00000 11111	00000 00000 11111	11111 11111 11111	11111 11111 11111	11111 11111 11111	100 010 001

Fig. 1. Circulant structure of a 2-(63,31,15) design with automorphisms of order 5.

these cases by two different algorithms [26]. For this particular problem, the construction of the solutions for M is computationally more time-consuming than the next stage of extending them to 2-(63,31,15) designs. In three of these cases there are no orbit matrices at all - $((b, b^T), (b, c^T), (b, d^T))$. In cases (c, d^T) and (d, d^T) we did not filter away all the equivalent matrices as it was faster to extend them to designs. We construct the following number of inequivalent orbit matrices: (a, a^T)- 2616, (a, b^T)- 4801, (a, c^T)- 69 581, (a, d^T)- 69 581, (b, b^T)- 0, (b, c^T)- 0, (b, d^T)- 0, (c, c^T)- 87 216, (c, d^T)- at least 90 000 and (d, d^T)- at least 90 000.

2.4. On 2-(63,31,15) designs invariant under the dihedral group of order 10

The dihedral group of order 10 (D_{10}) is the group of symmetries of a regular pentagon, including the four rotations $(1, 2, 3, 4, 5)$, $(1, 3, 5, 2, 4)$, $(1, 4, 2, 5, 3)$ and $(1, 5, 4, 3, 2)$, the five reflections $(1)(2, 5)(3, 4)$, $(1, 3)(2)(4, 5)$, $(1, 5)(2, 4)(3)$, $(1, 2)(3, 5)(4)$ and $(1, 4)(2, 3)(5)$, and the identity$(1)(2)(3)(4)(5)$. The group is generated by any pair of one rotation and one reflection, for instance by $(1, 2, 3, 4, 5)$ and $(1, 5)(2, 4)(3)$.

There are 31 circulant matrices of order 5. If we apply the same D_{10} rotation both to the rows, and to the columns of any of these circulants, the circulant remains unchanged. By a cyclic shift of rows or columns any circulant matrix of order 5 can be transformed into a circulant matrix, which is symmetric via the main diagonal (and as it is circulant, it is symmetric via the second diagonal too). There are 7 such symmetric matrices:

$$\begin{matrix}1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{matrix}\qquad\begin{matrix}0&0&1&1&0\\0&0&0&1&1\\1&0&0&0&1\\1&1&0&0&0\\0&1&1&0&0\end{matrix}\qquad\begin{matrix}0&1&0&0&1\\1&0&1&0&0\\0&1&0&1&0\\0&0&1&0&1\\1&0&0&1&0\end{matrix}$$

$$\begin{matrix}1&0&1&1&0\\0&1&0&1&1\\1&0&1&0&1\\1&1&0&1&0\\0&1&1&0&1\end{matrix}\qquad\begin{matrix}1&1&0&0&1\\1&1&1&0&0\\0&1&1&1&0\\0&0&1&1&1\\1&0&0&1&1\end{matrix}\qquad\begin{matrix}0&1&1&1&1\\1&0&1&1&1\\1&1&0&1&1\\1&1&1&0&1\\1&1&1&1&0\end{matrix}\qquad\begin{matrix}1&1&1&1&1\\1&1&1&1&1\\1&1&1&1&1\\1&1&1&1&1\\1&1&1&1&1\end{matrix}$$

If we apply the same D_{10} reflection both to the rows, and to the columns of any of these symmetric circulants, the circulant remains unchanged. If a circulant is not symmetric, for each D_{10} reflection applied on the rows, there is another different D_{10} reflection, which can be applied on the columns such that the circulant remains unchanged. Consider as an example the following circulant matrix

$$\begin{matrix}0&1&0&1&0\\0&0&1&0&1\\1&0&0&1&0\\0&1&0&0&1\\1&0&1&0&0\end{matrix}$$

It remains unchanged by the following five pairs of row (r) and column (c) permutations: r $(1)(2, 5)(3, 4)$, c $(1, 5)(2, 4)(3)$; r $(1, 3)(2)(4, 5)$, c $(1, 2)(3, 5)(4)$; r $(1, 5)(2, 4)(3)$, c $(1, 4)(2, 3)(5)$; r $(1, 2)(3, 5)(4)$, c $(1)(2, 5)(3, 4)$; r $(1, 4)(2, 3)(5)$, c $(1, 3)(2)(4, 5)$.

Consider the circulant structure of a 2-(63,31,15) design with automorphisms of order 5, which was discussed in the previous subsection (see also Fig. 1). All circulants are invariant under the same pairs of row and column D_{10} rotations, which actually make up the automorphisms of order five of the whole design.

By permutations of rows and columns of the incidence matrix of the design (such that rotations of the circulants are realized), we can make all the circulants in one circulant row and one circulant column symmetric. Namely, without loss of generality, we will consider an incidence matrix for which $a_{1,j}$ and $a_{i,1}$ are symmetric circulants, $i, j = 1, 2, \ldots, 12$.

Suppose we permute the rows of this incidence matrix of the design by a permutation φ, which acts on the first five points (on which the symmetric circulant row $a_{1,j}$ is) as one of the D_{10} reflections, for instance as $(1, 5)(2, 4)(3)$. The 12 circulants on these rows will only be reconstructed if the same D_{10} reflection is applied on their columns, i.e. if on the columns of the incidence matrix we apply $(1, 5)(2, 4)(3)(6, 10)(7, 9)(8)\ldots(56, 60)(57, 59)(58)(61)(62)(63)$.

Table 1
Order of the automorphism group of Hadamard 2-(63,31,15) designs invariant under the dihedral group of order 10

Order of the autom. group	Selfdual	Not selfdual	All
$10 = 10$	48	5576	5624
$20 = 10.2$	17	1316	1333
$30 = 10.3$	3	144	147
$40 = 10.2^2$	–	74	74
$60 = 10.3.2$	15	254	269
$120 = 10.3.2^2$	10	52	62
$160 = 10.2^4$	–	6	6
$180 = 10.3^2.2$	–	4	4
$320 = 10.2^5$	3	658	661
$360 = 10.3^2.2^2$	1	2	3
$640 = 10.2^6$	–	60	60
$960 = 10.3.2^5$	–	20	20
$1920 = 10.3.2^6$	3	42	45
$5760 = 10.3^2.2^6$	–	2	2
$10\,240 = 10.2^{10}$	–	2	2
$15\,360 = 10.3.2^9$	1	–	1
$30\,720 = 10.3.2^{10}$	1	4	5
$92\,160 = 10.3^2.2^{10}$	1	4	5
$1\,105\,920 = 10.3^3.2^{12}$	–	4	4
$30\,965\,760 = 10.7.3^3.2^{14}$	–	2	2
$20\,158\,709\,760 = 10.31.7^2.3^4.2^{14}$	1	–	1
All	104	8226	8330

After this column permutation the symmetric circulants $a_{i,1}$ of the first circulant column will remain unchanged if $\varphi = (1,5)(2,4)(3)(6,10)(7,9)(8)\ldots(56,60)(57,59)(58)(61)(62)(63)$. If so, then $(1,5)(2,4)(3)$ is actually applied on both the rows and columns of all the circulants $a_{i,j}$, $i, j = 1, 2, \ldots, 12$, and their circulant structure will only be preserved if they are all symmetric. In that case the whole design is invariant under D_{10} and its dihedral group of automorphisms is generated by the automorphism α of order 5 and the automorphism φ of order 2.

3. Construction of 2-(63,31,15) designs invariant under the dihedral group of order 10

We next extend the solutions for M to 2-(63,31,15) designs by replacing the elements of orbit matrices by symmetric circulants of order 5. The symmetry determines the automorphism φ of order 2. Most orbit matrices are not extendable to designs, that is why for this particular problem, the construction of matrices is computationally more difficult. Numbers of matrices, which are extendable to designs: (a, a^{T})- 139, (a, b^{T})- 114, (a, c^{T})- 544, (a, d^{T})- 542, (c, c^{T})- 367, (c, d^{T})- 345 and (d, d^{T})- 57.

We easily partition the constructed designs into equivalence classes such that two designs of one and the same class can be transformed into each other by permutations transforming the point/block orbits with respect to automorphism of order 5 into point/block orbits. We then calculate automorphism group orders, which are presented in Table 1. As far as none of the orders is divisible by 25 (none of the designs has more automorphisms of order 5 except the constructive ones), these are actually isomorphism classes.

In total 8330 nonisomorphic 2-(63,31,15) designs were obtained (104 selfdual), from (a, a^{T})- 398 (27 selfdual), (a, b^{T})- 798, (a, c^{T})- 2680, (a, d^{T})- 2680, (c, c^{T})- 841(61 selfdual), (c, d^{T})- 852 and (d, d^{T})- 80(16 selfdual).

4. Equivalence classes and automorphism groups of the corresponding Hadamard matrices of order 64

To the incidence matrix of each 2-(63,31,15) design we add an all-one row and an all-one column (we denote them row 0 and column 0), and replace 0 entries by -1 thus constructing the corresponding Hadamard matrix of order 64.

Applying to each of these matrices row and column negations, we next transform row i ($i = 0, 61, 62, 63$) and column j ($j = 0, 61, 62, 63$) into an all-one row/column. We then remove the all-one row and column, replace -1 entries by 0 and obtain a Hadamard 2-(63,31,15) design. This way we obtain sixteen 2-(63,31,15) designs with constructive automorphisms and extendable to the same Hadamard matrix. We compare these 16 design collections to filter away equivalent Hadamard matrices. Thus 1691 Hadamard matrices remain.

Let H and $\bar{H}$ be two Hadamard matrices of order n, such that the elements of the first one equal the elements of the second multiplied by -1. Denote by H^* the matrix $H^* = \begin{pmatrix} H & \bar{H} \\ \bar{H} & H \end{pmatrix}$. The order of the full automorphism group of a Hadamard matrix H is the same as the order of the full automorphism group of the matrix H^*, and two Hadamard matrices H_1 and H_2 are equivalent if the matrices H_1^* and H_2^* are equivalent [16,28,38].

For the remaining 1691 Hadamard matrices we calculate the following invariants: for each row (column) i of H^* we compute the vector $(m_0, m_1, \ldots, m_{32})$, where m_s is the number of triples of rows (columns) j, k, l, different from i and such that there are s columns containing 1s in each of the rows i, j, k, l. There are 1679 different invariants. For the Hadamard matrices, which have the same invariants, we examine all the Hadamard 2-designs, corresponding to them, and establish that in all these cases they are different. This proves the inequivalence of the 1691 Hadamard matrices of order 64 (39 self-dual ones and 826 pairs of dual matrices). We present in Table 2 their classification with respect to the automorphism groups, which we calculated by Bouyukliev's program [3]. We also used the latter programme to check in parallel the inequivalence of these Hadamard matrices.

5. Line spreads and the corresponding 2-(64,16,5) designs

The following Rahilly's construction [29] relates any $2-(16m, 4m, (4m-1)/3)$ affine design d with a Hadamard $2-(16m-1, 8m-1, 4m-1)$ design D whose dual D^* has a line spread consisting of lines of size 3.

Construction 1. Choose any point w of d, and consider as points of D all points of d except w. Each parallel class C of d gives three blocks of D as follows. Let B_0 be the block of d from the parallel class C that contains w. For any block B of d such that $B \in C$ and $w \notin B$, define $B \cup B_0 - \{w\}$ to be a block of D.

Conversely, if D is a symmetric $2-(16m-1, 8m-1, 4m-1)$ design whose dual design D^* admits a spread S of lines of size 3, we can define an affine $2-(16m, 4m, (4m-1)/3)$ design d as follows.

Construction 2. The point set of d consists of the points of D plus one new point w. Let B_1, B_2, B_3 be three blocks of D that correspond to a line in D^* from the spread S. Let $M = B_1 \cap B_2 \cap B_3$. Define a parallel class C of d consisting of the four blocks $B'_1 = B_1 - M$, $B'_2 = B_2 - M$, $B'_3 = B_3 - M$, $B'_4 = M \cup \{w\}$.

A generalization of both constructions may also be found in [18].

Consider the 2-ranks of D and d. Let A be the incidence matrix of D with an additional all-one row. Let a be the incidence matrix of d. As columns of A are sums (over GF(2)) of columns of a, the 2-rank of D is at most as great as the 2-rank of d [37].

Below we restrict D and D^* to be 2-(63,31,15) designs, and d a 2-(64,16,5) design. There are two geometric designs with these parameters, i.e. a 2-(63,31,15) corresponding to PG(5,2), and a 2-(64,16,5) corresponding to AG(3,4). Three 2-(64,16,5) of minimal rank 16 are known, the two of them obtainable from line spreads of PG(5,2). We want to see if more such designs can be obtained from the Hadamard designs we construct.

Since we are interested in affine 2-(64,16,5) designs of minimal rank (the minimal known rank is 16), we first check the 2-rank of the 2-(63,31,15) designs we obtain, and establish that there are 920 designs of 2-rank at most 16. Among them 1 design of rank $7(PG(5,2))$, 6 of rank 8, 13 of rank 11, 151 of rank 12, 111 of rank 13, 16 of rank 14, 36 of rank 15, and 586 of rank 16.

We check for each of these designs whether they possess line spreads, from which 2-(64,16,5) designs of rank at most 16 are constructed. We obtain two such minimal rank 2-(64,16,5) designs from the rank 7 Hadamard 2-design, and one from a rank 8 Hadamard 2-design (with automorphism group order 1105 920), i.e. all the known examples, but no new one. A brief description of the way we do this follows.

Computing the rank R of the Hadamard design, we also find a system S of R linearly independent vectors (columns of A) of length 64. We then create a list of all the weight 16 vectors of length 64, which are obtained as intersection of three columns of A corresponding to a line of size 3 in D^*. There is a one-to-one correspondence between these vectors and the lines.

The maximum number of lines is 651 (attained by the geometric design of rank 7). For each block of D (point of D^*), we calculate the number of lines containing it (at most 31 for these parameters), and we sort the blocks of D (points of D^*) with respect to this number. If some point of D^* is in no line of size 3, a spread is impossible.

Table 2
Order of the full automorphism group of the Hadamard matrices

Order of the autom. group	Selfdual	Not selfdual	All
$20 = 10.2$	1	32	33
$40 = 10.2^2$	3	210	213
$60 = 10.3.2$	0	32	32
$80 = 10.2^3$	2	338	340
$120 = 10.3.2^2$	6	14	20
$160 = 10.2^4$	2	238	240
$240 = 10.3.2^3$	0	48	48
$320 = 10.2^5$	0	84	84
$360 = 10.3^2.2^2$	0	8	8
$480 = 10.3.2^4$	4	74	78
$640 = 10.2^6$	0	60	60
$960 = 10.3.2^5$	1	44	45
$1280 = 10.2^7$	1	116	117
$1920 = 10.3.2^6$	1	30	31
$2560 = 10.2^8$	1	92	93
$2880 = 10.3^2.2^5$	0	2	2
$3840 = 10.3.2^7$	1	26	27
$5120 = 10.2^9$	0	34	34
$5760 = 10.3^2.2^6$	2	10	12
$7680 = 10.3.2^8$	1	24	25
$10\,240 = 10.2^{10}$	0	12	12
$15\,360 = 10.3.2^9$	2	14	16
$20\,480 = 10.2^{11}$	0	2	2
$23\,040 = 10.3^2.2^8$	1	0	1
$30\,720 = 10.3.2^{10}$	0	4	4
$40\,960 = 10.2^{12}$	0	8	8
$61\,440 = 10.3.2^{11}$	2	2	4
$81\,920 = 10.2^{13}$	0	12	12
$122\,880 = 10.3.2^{12}$	2	6	8
$163\,840 = 10.2^{14}$	0	16	16
$184\,320 = 10.3^2.2^{11}$	1	0	1
$245\,760 = 10.3.2^{13}$	2	12	14
$327\,680 = 10.2^{15}$	0	4	4
$491\,520 = 10.3.2^{14}$	1	12	13
$737\,280 = 10.3^2.2^{13}$	0	4	4
$983\,040 = 10.3.2^{15}$	0	12	12
$2\,621\,440 = 10.2^{18}$	0	2	2
$2\,949\,120 = 10.3^2.2^{15}$	0	2	2
$3\,932\,160 = 10.3.2^{17}$	0	2	2
$7\,864\,320 = 10.3.2^{18}$	0	4	4
$566\,231\,040 = 10.3^3.2^{21}$	0	2	2
$754\,974\,720 = 10.3^2.2^{23}$	1	0	1
$9059\,696\,640 = 10.3^3.2^{25}$	0	2	2
$15\,854\,469\,120 = 10.7.3^3.2^{23}$	0	2	2
$165\,140\,150\,353\,920 = 10.31.7^2.3^4.2^{27}$	1	0	1
All	39	1652	1691

We construct the spread by backtrack search. At the beginning there are no lines in it. At each step we choose the next line to contain the yet to be added point of D^*, which is in the least number of lines. Then we check if the weight 16 vector, corresponding to this line, is linearly independent on the vectors in S, and if it is, we add it to S. If the rank of S becomes greater than 16, we remove the latest added line (and the corresponding vector from S), and try the next possible one.

Acknowledgments

The authors are grateful to professor Vladimir Tonchev from Michigan Technological University, USA, for focusing our attention to this problem, and for several important advices on it, and on the content of this manuscript.

The second author is partially supported by the Bulgarian National Science Fund under Contract No. MM 1405.

References

[1] E.F. Assmus Jr., J.D. Key, Designs and their Codes, in: Cambridge Tracts in Mathematics, vol. 103, Cambridge University Press, 1992.
[2] Th. Beth, D. Jungnickel, H. Lenz, Design Theory, Cambridge University Press, 1993.
[3] I. Bouyukliev, About the code equivalence, in: T. Shaska, W.C. Huffman, D. Joyner, V. Ustimenko (Eds.), Advances in Coding Theory and Cryptology, in: Series on Coding Theory and Cryptology, vol. 3, World Scientific Publishing Co. Pte. Ltd., 2007, pp. 126–151.
[4] I. Bouyukliev, V. Fack, J. Winne, Hadamard matrices of order 36 and double-even self-dual [72, 36, 12] codes, in: Proceedings of EUROCOMB'2005, Berlin, Germany, 2005, pp. 93–98.
[5] A.R. Camina, A survey of the automorphism groups of block designs, J. Combin. Designs 2 (2) (1994) 79–100.
[6] R. Craigen, Hadamard matrices and designs, in: The CRC Handbook of Combinatorial Designs, CRC Press, Boca Raton, FL, 1996, pp. 370–377.
[7] R. Craigen, W. Wallis, Hadamard matrices: 1893–1993, Congressus Numeratum 97 (1993) 99–129.
[8] R. Craigen, H. Kharaghani, Weaving Hadamard matrices with maximum excess and classes with small excess, J. Combin. Designs 12 (2004) 233–255.
[9] D. Crnković, On some symmetric designs with classical parameters, Acta Math. Acad. Paedagog. Nyházi 22 (1) (2006) 5–18. (electronic) http://www.emis.de/journals/AMAPN.
[10] W. Feit, Automorphisms of symmetric ballanced incomplete block designs, Math. Z. 118 (1970) 40–49.
[11] S. Georgiou, C. Koukouvinos, J. Seberry, Hadamard matrices, orthogonal designs and construction algorithms, in: DESIGNS 2002, Further Computational and Constructive Design Theory, Kluwer, 2003, pp. 133–205.
[12] S. Georgiou, C. Koukouvinos, S. Stylianou, On good matrices, skew Hadamard matrices and optimal designs, Comput. Statist. Data Anal. 41 (1) (2002) 171–184.
[13] S. Georgiou, I. Kotsireas, C. Koukouvinos, Astronomical Bounds for finding inequivalent Hadamard Matrices, Mathematics of Computer Algebra and Analysis, University of Waterloo, Waterloo, Ontario, June 4–6, 2005.
[14] N. Hamada, On the p-rank of the incidence matrix of a balanced or partially balanced incomplete block design and its applications to error-correcting codes, Hiroshima Math. J. 3 (1973) 153–226.
[15] M. Harada, C. Lam, V.D. Tonchev, Symmetric (4, 4)-nets and generalized Hadamard matrices over groups of order 4, Designs Codes Cryptogr. 34 (2005) 71–87.
[16] N. Ito, On Hadamard groups, J. Algebra 168 (1994) 981–987.
[17] N. Ito, J.S. Leon, J.Q. Longyear, Classification of 3-(24, 12, 5) designs and 24-dimensional Hadamard matrices, J. Combin. Theory, Ser. A 31 (1981) 66–93.
[18] A.N. Al-Kenani, V.C. Mavron, Maximal arc partitions of designs, Discrete Math. (in press).
[19] H. Kimura, Hadamard matrices of order 28 with automorphism groups of order 2, J. Combin. Theory, Ser. A 43 (1986) 98–102.
[20] H. Kimura, New Hadamard matrix of order 24, Graphs Combin. 5 (1989) 235–242.
[21] H. Kimura, Classification of Hadamard matrices of order 28, Discrete Math. 133 (1994) 171–180.
[22] I. Kotsireas, Ch. Koukouvinos, J. Seberry, Hadamard ideals and Hadamard matrices with two circulant cores, European J. Combin. 27 (5) (2006) 658–668.
[23] C. Lam, S. Lam, V.D. Tonchev, Bounds on the number of affine, symmetric and Hadamard designs and matrices, J. Combin. Theory Ser. A 92 (2000) 186–196.
[24] C. Lam, S. Lam, V.D. Tonchev, Bounds on the number of Hadamard designs of even order, J. Combinatorial Designs 9 (2001) 363–378.
[25] E.S. Lander, Symmetric Designs: An Algebraic Approach, in: London Math. Soc. Lecture Note Ser., vol. 74, Cambridge University Press, Cambridge, 1983.
[26] Z. Mateva, An algorithm for constructing tactical decompositions for 2-(63, 31, 15) designs invariant under the dihedral group of order 10, in: Proceedings of Intern. Scientific Conference, Informatics in the scentific knowledge, Varna, Bulgaria, 2006, pp. 351–357.
[27] V.C. Mavron, T. McDonough, V.D. Tonchev, On affine designs and Hadamard designs with line spreads, Discrete Math. (in press).
[28] B. McKay, Hadamard equivalence via graph isomorphism, Discrete Math. 27 (1979) 213–214.
[29] A. Rahilly, On the line structure of designs, Discrete Math. 92 (1991) 291–303.
[30] J. Seberry, M. Yamada, Hadamard matrices, sequences, and block designs, in: J.H. Dinitz, D.R. Stinson (Eds.), Contemporary Design Theory, A Collection of Surveys, Wiley, 1992, pp. 431–560.
[31] E. Spence, Classification of Hadamard matrices of orders 24 and 28, Discrete. Math. 140 (1995) 185–243.
[32] E. Spence, Regular two-graphs on 36 vertices, Linear Algebra Appl. 226–228 (1995) 459–497.
[33] V.D. Tonchev, Hadamard matrices of order 28 with automorphisms of order 7, J. Combin. Theory, Ser. A 40 (1985) 62–81.
[34] V.D. Tonchev, Hadamard matrices of order 36 with automorphisms of order 17, Nagoya Math. J. 104 (1986) 163–174.
[35] V.D. Tonchev, Quasi-symmetric 2-(31, 7, 7) designs and a revision of Hamadas conjecture, J. Combin. Theory, Ser. A 42 (1986) 104–110.
[36] V.D. Tonchev, Combinatorial Configurations, Longman Scientific and Technical, New York, 1988.
[37] V.D. Tonchev, in: A. Hulpke, R. Liebler, T. Penttila, A. Seress (Eds.), On Affine Designs and GMW Difference Sets, Finite Geometries, Groups, and Computation, Walter de Gruyter, Berlin, 2006, pp. 237–245.
[38] S. Topalova, Classification of Hadamard matrices of order 44 with automorphisms of order 7, Discrete Math. 260 (2003) 275–283.